

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-338985  
 (43)Date of publication of application : 10.12.1999

(51)Int.CI. G06K 17/00  
 G06K 19/07  
 G06K 19/10  
 G06K 19/073

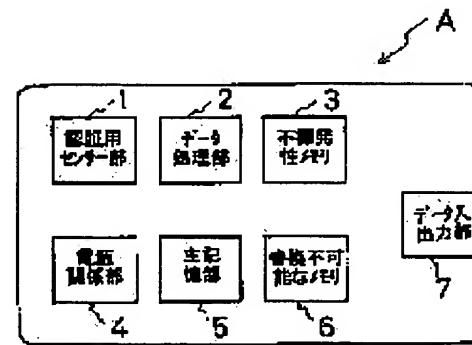
(21)Application number : 10-144885 (71)Applicant : NIPPON TELEGR & TELEPH CORP  
 <NTT>  
 (22)Date of filing : 26.05.1998 (72)Inventor : TANAKA KEIJI  
 TATEMICHU HIDETOSHI  
 ISOMURA YOSHINORI  
 KATO KIKUJI

## (54) SECURITY LEVEL SETTING AND DISCRIMINATION METHOD, IC CARD AND ITS USE

### (57)Abstract:

PROBLEM TO BE SOLVED: To provide a discrimination method capable of setting and discriminating the security level corresponding to service contents and leaving a past service utilization history, and to provide an IC card and its use.

SOLUTION: This IC card A is provided with a sensor part 1 for authentication for reading a certain intrinsic physical feature, a data processing part 2, a nonvolatile memory 3 capable of storing and additionally writing data relating to a service utilization right, a power relation part 4 provided with a terminal for power supply or a power supply part or the like for receiving power supply, a main memory part 5, a non-rewritable memory 6 for individually holding the data for individual authentication, an individual ID and a card ID and a data input/output part 7.



### LEGAL STATUS

[Date of request for examination] 25.01.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

**THIS PAGE BLANK (USPTO)**

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-338985

(43)公開日 平成11年(1999)12月10日

(51)Int.Cl.<sup>a</sup>  
G 0 6 K 17/00

識別記号

F I  
G 0 6 K 17/00

T  
B  
V  
N  
R

19/07  
19/10

19/00

審査請求 未請求 請求項の数45 OL (全 22 頁) 最終頁に続く

(21)出願番号 特願平10-144885

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(22)出願日 平成10年(1998)5月26日

(72)発明者 田中 敬二

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72)発明者 立道 英俊

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72)発明者 磯村 嘉伯

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(74)代理人 弁理士 菅 隆彦

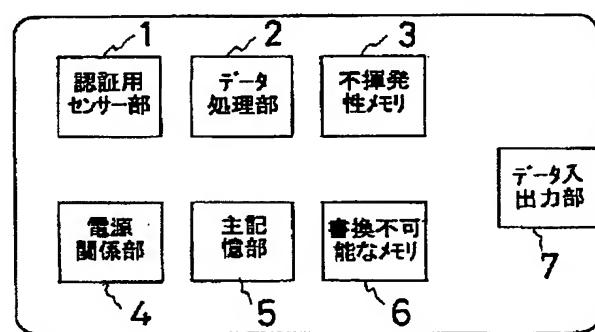
最終頁に続く

(54)【発明の名称】セキュリティレベル設定判別方法とICカード及びその使用方法

(57)【要約】

サービス内容に応じてセキュリティレベルを設定判別でき、且つ過去のサービス利用履歴を残すことが可能な判別方法、ICカード及びICカード使用方法の提供。

【解決手段】ある固有の身体的特徴を読み取る為の認証用センサー部1と、データ処理部2と、サービス利用権に関わるデータを記憶させ、且つ追加書き込むできる不揮発性メモリ3と、電源供給を受けるための電源供給用端子又は電源供給部等を有する電源関係部4と、主記憶部5と、個人認証用データ、個人ID、カードIDが個別に保持する為の書換不可能なメモリ6と、データ入出力部7とを有することの特徴。



## 【特許請求の範囲】

【請求項1】所望のサービスを要求するに当たり、  
予め設定したセキュリティレベルに照して必要と判別された場合に限り個人認証処理を実行する、  
ことを特徴とするセキュリティレベル設定判別方法。

【請求項2】所望のサービスを要求するに当たり、  
当該要求するサービスの内容に応じて個人認証必要性に関する情報を予めサービス要求手段に記憶させておき、  
サービス要求の際に前記サービス要求手段内の個人認証必要性に関する情報に基いて個人認証確認の有無を判別する、  
ことを特徴とするセキュリティレベル設定判別方法。

【請求項3】複数のサービス内から所望のサービスを要求するに当たり、  
当該要求する各サービスに応じて個人認証必要性に関する情報を予め一のサービス要求手段に記憶させておき、  
サービス要求の際に前記サービス要求手段内の個人認証必要性に関する情報に基いて個人認証の有無を判別する、  
ことを特徴とするセキュリティレベル設定判別方法。

【請求項4】前記個人認証必要性に関する情報は、  
サービスID、サービス提供条件、個人認証の要不要情報を含む、  
ことを特徴とする請求項2又は3に記載のセキュリティレベル設定判別方法。

【請求項5】前記個人認証必要性に関する情報は、  
サービス毎の初期設定後、任意に追加書き込まれる、  
ことを特徴とする請求項2、3又は4に記載のセキュリティレベル設定判別方法。

【請求項6】サービス内容に応じて個人認証に必要なセキュリティレベルを予め記憶する手段を有する、ことを特徴とするICカード。

【請求項7】認証用センサー部、データ処理部、不揮発性メモリ、電源関係部、主記憶部、書換不能なメモリ及びデータ入出力部を有するICカードにおいて、  
前記不揮発性メモリ内に予め記憶させたサービス使用権情報に基づき前記認証用センサー部で検出したある固有の身体的特徴との照合一致を前記データ処理部が判定する一連の機能を持たせる、  
ことを特徴とするICカード。

【請求項8】前記サービス使用権情報は、  
サービスID、サービス提供条件及び前記認証用センサー部によるICカード使用者のある固有の身体的特徴情報である、  
ことを特徴とする請求項7に記載のICカード。

【請求項9】前記サービス提供条件は、  
サービス受益期間、サービス受益回数の何れか又は双方である、  
ことを特徴とする請求項8に記載のICカード。

【請求項10】前記書換不可能なメモリは、

個人認証用データ、個人ID、カードIDを記憶する機能を有する、

ことを特徴とする請求項7、8又は9に記載のICカード。

【請求項11】前記書換不可能なメモリは、  
物理的構造上書き換え不可能なメモリである、  
ことを特徴とする請求項7、8、9又は10に記載のICカード。

【請求項12】前記書換不可能なメモリは、  
データ構造上書き換えることが不可能なメモリである、  
ことを特徴とする請求項7、8、9又は10に記載のICカード。

【請求項13】前記不揮発性メモリは、  
追加書き込み自在とする、  
ことを特徴とする請求項7、8、9、10、11又は12に記載のICカード。

【請求項14】前記電源関係部は、  
電源供給部を有する、  
ことを特徴とする請求項7、8、9、10、11、12又は13に記載のICカード。

【請求項15】前記電源関係部は、  
電源供給を受けるための電源供給用端子を有する、  
ことを特徴とする請求項7、8、9、10、11、12又は13に記載のICカード。

【請求項16】前記データ処理部は、  
前記不揮発性メモリ内に記憶され情報を検索し定処理する機能を具備する、  
ことを特徴とする請求項7、8、9、10、11、12、13、14又は15に記載のICカード。

【請求項17】前記データ処理部は、  
前記主記憶部、前記書き不可能なメモリ及び前記不揮発性メモリにある情報を検索しそれぞれ定処理する機能をさらに具備する、  
ことを特徴とする請求項7、8、9、10、11、12、13、14、15又は16に記載のICカード。

【請求項18】前記ICカードは、  
ヒューマンインターフェイス部をもさらに具備する、  
ことを特徴とする請求項7、8、9、10、11、12、13、14、15、16又は17に記載のICカード。

【請求項19】前記ヒューマンインターフェイス部は、  
人手入力自在な入力部を具備する、  
ことを特徴とする請求項18に記載のICカード。

【請求項20】前記ヒューマンインターフェイス部は、  
外部認識自在な出力部を具備する、  
ことを特徴とする請求項18に記載のICカード。

【請求項21】前記ヒューマンインターフェイス部は、  
前記入力部と前記出力部を併せて具備することを特徴とする請求項18に記載のICカード。

【請求項22】前記入力部は、

3

受益サービス選択機能を有する、  
ことを特徴とする請求項19又は21に記載のICカード。

【請求項23】前記入力部は、  
手書き入力手段である、  
ことを特徴とする請求項19、21又は22に記載のICカード。  
【請求項24】前記手書き入力手段は、  
入力された情報を解読しコード化する手書き入力認識機能を具備する、  
ことを特徴とする請求項23に記載のICカード。

【請求項25】前記入力は、  
文字入力、図形入力若しくは絵入力又はそれらの組合せである、  
ことを特徴とする請求項24に記載のICカード。

【請求項26】前記入力部は、  
音入力手段である、  
ことを特徴とする請求項19又は21に記載のICカード。

【請求項27】前記音入力手段は、  
入力された音を解読しコード化する音声認識機能を有する、  
ことを特徴とする請求項26に記載のICカード。

【請求項28】前記出力部は、  
表示手段、LEDランプ若しくは音出力手段又はこれらの組合せ手段である、  
ことを特徴とする請求項20又は21に記載のICカード。

【請求項29】前記音出力手段は、  
コード化されたコードデータを音出力する音合成機能を有する、  
ことを特徴とする請求項28に記載のICカード。

【請求項30】前記入力部と前記出力部は、  
一体化された音声入出力手段である、  
ことを特徴とする請求項21に記載のICカード。

【請求項31】前記データ入出力部は、  
前記ICカードに対応する端末との通信の為の無線通信機能を具備する、  
ことを特徴とする請求項7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29又は30に記載のICカード。

【請求項32】前記無線通信機能は、  
ISO10536、ISO14443、ISO15693、PHS方式、IMT2000に準拠する、  
ことを特徴とする請求項31に記載のICカード。

【請求項33】前記データ入出力部は、  
暗号化されたデータを入出力自在とする、  
ことを特徴とする請求項7、8、9、10、11、12、13、14、15、16、17、18、19、20に記載のICカード。

0、21、22、23、24、25、26、27、28、29、30、31又は32に記載のICカード。

【請求項34】前記ICカードは、  
電源のON/OFFを制御可能とするスイッチ手段を具備する、  
ことを特徴とする請求項7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32又は33に記載のICカード。

【請求項35】前記スイッチ手段は、  
前記ICカード外部からの信号を受信し、電源供給をON状態にする機能を有する、  
ことを特徴とする請求項34に記載のICカード。

【請求項36】前記認証用センサー部は、  
指紋読取りセンサー、手書き読取りセンサー、音声センサー若しくは虹彩読取りセンサー、又は前記センサーを組み合わせた複合センサーである、  
ことを特徴とする請求項7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32、33、34又は35に記載のICカード。

【請求項37】前記認証用センサー部は、  
前記ICカードを把持した際に自動的に認証を実行自在な配置とする、  
ことを特徴とする、請求項7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32、33、34、35又は36に記載のICカード。

【請求項38】前記配置は、  
ICカードの把持する指接触にて自発的に指紋認証処置を実行せしめるよう、当該ICカードの表面の大部分を指紋センサーにて占有せしめる、  
ことを特徴とする請求項37に記載のICカード。

【請求項39】請求項7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32、33、34、35、36、37又は38に記載のICカードと、当該ICカードを処理可能な端末及び当該端末に接続可能なサービスセンタとからなるICカードサービス利用システムの利用に当たり、

最初だけ、前記サービスセンタに前記ICカードを前記端末を介し接続して新規登録を行ってから、前記ICカード及び前記サービスセンタ相互間の利用環境設定をその都度行うことにより、  
所望のサービスを当該ICカードと当該サービスセンタ間で要求提供できる、

ことを特徴とする I C カード使用方法。

【請求項 4 0】前記新規登録は、

前記 I C カードによる個人認証の結果を考慮して行い、前記端末から前記サービスセンタに送信された前記個人 I D に基づき事前に届けられた使用不可の個人 I D に該当するかどうかの当該サービスセンタでの利用可能性を判断した結果に基づき、

利用可能の場合には、

前記サービスセンタに前記個人 I D の登録を行い、

前記端末は当該サービスセンタから送信された前記サービス I D を前記 I C カードに送信し、

前記 I C カードの不揮発性メモリに当該サービス I D を記憶する、

以上一連のステップを踏んで実行される、

ことを特徴とする請求項 3 9 に記載の I C カード使用方法。

【請求項 4 1】前記利用環境設定は、

前記 I C カードによる個人認証の結果を考慮して行い、サービス受益者が前記端末又は前記 I C カードに対して前記サービス使用権情報に関する設定後、

当該設定された前記サービス利用環境を前記個人 I D と共に前記サービスセンタに送信し、

当該サービスセンタは送信された情報を確認した後に当該サービスセンタ内に記憶させ、

前記端末又は前記 I C カードは、当該 I C カードの前記不揮発性メモリに前記サービスセンタに記憶させた情報と同一の情報を書き込み登録させる、

以上一連のステップを踏んで実行される、

ことを特徴とする請求項 3 9 又は 4 0 に記載の I C カード使用方法。

【請求項 4 2】前記端末は、

サービス要求者からの前記個人 I D の投入があると、当該サービス要求者に対して個人認証必要性を前記サービス使用権情報から判定し、

当該判定の結果必要な場合のみ、前記 I C カード内の前記認証用センサ部によりある固有の前記身体的特徴検出処理を行った後、処理結果を前記個人認証用データと照合することにより個人認証判定を行い、

当該個人認証判定が不要又は正の場合には、

前記サービスセンタに前記端末から前記個人 I D 及びサービス I D を送信し、

当該サービスセンタは送信情報を確認後、サービス提供可能と判断した場合には要求されたサービスを提供する、

以上一連のステップを踏んで処理する、

ことを特徴とする請求項 4 1 に記載の I C カード使用方法。

【請求項 4 3】前記 I C カードは、

前記端末より前記サービス I D を受信すると、個人認証必要性を前記サービス使用権情報から判定し、

当該判定の結果必要な場合のみ、前記認証用センサ部によりある固有の前記身体的特徴検出処理を行った後、当該処理結果を前記個人認証用データと照合させることにより個人認証判定を行い、

当該個人認証判定が不要又は正の場合には、

サービス利用環境の設定からサービスの提供か否かを判断し、

サービス提供可能と判断された場合には、サービス提供を行う、

10 以上一連のステップを踏んで処理する、  
ことを特徴とする請求項 4 1 に記載の I C カード使用方法。

【請求項 4 4】前記サービス提供可能との判断は、

前記 I C カード内の前記不揮発性メモリ及び前記サービスセンタにサービス提供実施に関するサービス提供情報の追加記憶を実行させる、

ことを特徴とする請求項 4 2 又は 4 3 に記載の I C カード使用方法。

【請求項 4 5】前記サービス提供情報は、

20 前記端末を介して当該端末と前記サービスセンタとが前記サービス I D 又は前記個人 I D を送受信する際に同時に送信され、当該サービス提供情報に関する送信された情報と自己が記憶している情報とが合致する否かを確認され、不一致の場合には、サービス提供を中止させる、  
以上一連のステップを踏んで実行させる、  
ことを特徴とする請求項 4 4 に記載の I C カード使用方法。

【発明の詳細な説明】

【0 0 0 1】

30 【発明の属する技術分野】本発明は、セキュリティレベルをサービス内容に応じて選択可能とするセキュリティレベル設定判別方法とその実施に直接使用する I C カード及び当該 I C カードを実質的に利用可能とする I C カードサービス利用システムの I C カード使用方法に関するものである。

【0 0 0 2】

【従来の技術】従来、 I C カードは、演算処理、主記憶部、 R OM 、不揮発性メモリ、データ入出力部から構成されている。そして、 I C カードを使用する際、カードに記憶された、例えばパスワードと外部装置に入力されたパスワードとを照合させることによりセキュリティ確認を行い、一致した場合のみサービスを受益できるしくみになっている。

【0 0 0 3】また、従来の I C カードには、正規の I C カード所有者と現に使用する者の一致確認を I C カード単体で行う機能を有していない。即ち、外部装置に入力するパスワードさえ知りさえすれば、 I C カード所有者に成りすまして、その I C カードを使用することが可能となるという問題を生じる。

50 【0 0 0 4】この問題を解決する手段として、 I C カー

ドに指紋、声紋等の身体的特徴を読取るセンサーをICカードに組み込むことが、例えば特開昭63-5309号公報に記載されている。

【0005】

【発明が解決しようとする課題】指紋、声紋その他の身体的特徴を読取るセンサーをICカードに組み込むことにより、セキュリティの高いICカードが実現できるものの、セキュリティが非常に高いサービスにのみ特化したカードとなり、個人認証を要しないサービスに対しても、個人認証を行わなければならないという問題を新たに生じる。即ち、認証可能なICカードにおいては必ずICカードで個人認証を行わないとサービスを受益できないことになり、サービスの授受において煩わしさを感じさせる。

【0006】また、個人認証を行うICカードにおいて万が一、本人認証用データが改ざんされ、不正なサービス利用を受けた場合、ICカードにおけるサービス利用履歴を監視できないと、永久に不正利用が続くという問題が生じる。

【0007】ここにおいて、本発明の解決すべき主要な目的は以下の通りである。即ち、本発明の第1の目的は、サービス内容に応じて個人認証必要性の有無を設定可能とするセキュリティレベル設定判別方法とICカード及びその使用方法を提供せんとするものである。

【0008】本発明の第2の目的は、過去のサービス利用履歴を残すことが可能なセキュリティレベル設定判別方法とICカード及びその使用方法を提供せんとするものである。

【0009】本発明の第3の目的は、必要に応じて極めて高い不正使用を防止するセキュリティレベル設定判別方法とICカード及びその使用方法を提供せんとするものである。

【0010】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなる。

【0011】

【課題を解決するための手段】本発明方法は、上記課題の解決に当たり、所望のサービスを要求する前に、予め要求するサービスの内容に応じて個人認証必要性に関する情報をサービス要求手段に記憶させておき、サービス要求の際に前記サービス要求手段内の必要性に関する情報に基いて個人認証確認の有無を判別するという手法を講じる特徴を有する。

【0012】本発明カードは、上記課題の解決に当たり、サービス内容に応じてサービス毎に個人認証確認の必要性の有無を予め記憶させるという手段を講じる特徴を有する。

【0013】本発明使用方法は、上記課題の解決に当たり、前記本発明カードと当該ICカードを処理可能な端末と当該端末に接続可能なサービスセンタとを有するシ

ステムの利用に当たり、所望のサービスに対して、予め前記サービスセンタと接続して新規登録を行うと共に、前記ICカード及び当該サービスセンタ相互間に利用環境設定をその都度行う必要性があるという手法を講じる特徴を有する。

【0014】更に、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法及び手段を採用することにより、前記目的を達成するようにならざる。

10 【0015】本発明方法の第1の特徴は、所望のサービスを要求するに当たり、予め設定したセキュリティレベルに照して必要と判別された場合に限り個人認証処理を実行してなるセキュリティレベル設定判別方法の構成採用にある。

【0016】本発明方法の第2の特徴は、所望のサービスを要求するに当たり、当該要求するサービスの内容に応じて個人認証必要性に関する情報を予めサービス要求手段に記憶させておき、サービス要求の際にサービス要求手段内の個人認証必要性に関する情報に基いて個人認証確認の有無を判別してなるセキュリティ設定判別方法の構成採用にある。

20 【0017】本発明方法の第3の特徴は、複数のサービス内から所望のサービスを要求するに当たり、当該要求する各サービスに応じて個人認証必要性に関する情報を予めサービス要求手段に記憶させておき、サービス要求の際にサービス要求手段内の個人認証必要性に関する情報に基いて個人認証の有無を判別してなるセキュリティレベル設定判別方法の構成採用にある。

【0018】本発明方法の第4の特徴は、上記本発明方法の第2又は第3の特徴における個人認証必要性に関する情報が、サービスID、サービス提供条件、個人認証の要否情報を含んでなるセキュリティレベル設定判別方法の構成採用にある。

30 【0019】本発明方法の第5の特徴は、上記本発明方法の第2、第3又は第4の特徴における個人認証必要性に関する情報が、サービス毎の初期設定後、任意に追加書き込まれてなるセキュリティレベル設定方法の構成採用にある。

【0020】本発明カードの第1の特徴は、サービス内容に応じて個人認証に必要なセキュリティレベルを予め記憶する手段を有してなるICカードの構成採用にある。

40 【0021】本発明カードの第2の特徴は、認証用センサー部、データ処理部、不揮発性メモリ、電源関係部、主記憶部、書換不能なメモリ及びデータ入出力部を有するICカードにおいて、不揮発性メモリ内に予め記憶させたサービス使用権情報に基づき認証用センサー部で検出したある固有の身体的特徴との照合一致を前記データ処理部が判定する一連の機能を持たせてなるICカードの構成採用にある。

【0022】本発明カードの第3の特徴は、上記本発明カードの第2の特徴におけるサービス使用権情報が、サービスID、サービス提供条件及び認証用センサー部によるICカード使用者のある固有の身体的特徴情報の有無であるICカードの構成採用にある。

【0023】本発明カードの第4の特徴は、上記本発明カードの第3の特徴におけるサービス提供条件が、サービス受益期間、サービス受益回数の何れか又は双方であるICカードの構成採用にある。

【0024】本発明カードの第5の特徴は、上記本発明カードの第2、第3又は第4の特徴における書換不可能なメモリが、個人認証用データ、個人ID、カードIDを記憶する機能を有してなるICカードの構成採用にある。

【0025】本発明カードの第6の特徴は、上記本発明カードの第2、第3、第4又は第5の特徴における書換不可能なメモリが、物理的構造上書き換え不可能なメモリであるICカードの構成採用にある。

【0026】本発明カードの第7の特徴は、上記本発明カードの第2、第3、第4又は第5の特徴における書換不可能なメモリが、データ構造上書き換えることが不可能なメモリであるICカードの構成採用にある。

【0027】本発明カードの第8の特徴は、上記本発明カードの第2、第3、第4、第5、第6又は第7の特徴における不揮発性メモリが、追加書き込み自在としてなるICカードの構成採用にある。

【0028】本発明カードの第9の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7又は第8の特徴における電源関係部が、電源供給部を有してなるICカードの構成採用にある。

【0029】本発明カードの第10の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7又は第8の特徴における電源関係部が、電源供給を受けるための電源供給用端子を有してなるICカードの構成採用にある。

【0030】本発明カードの第11の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7、第8、第9又は第10の特徴におけるデータ処理部が、不揮発性メモリ内に記憶され情報を検索し定処理する機能を具备してなるICカードの構成採用にある。

【0031】本発明カードの第12の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴におけるデータ処理部が、主記憶部、書き不可能なメモリ及び不揮発性メモリにある情報を検索しそれぞれ定処理する機能をさらに具备してなるICカードの構成採用にある。

【0032】本発明カードの第13の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7、第8、第9、第10、第11又は第12の特徴におけるICカードが、ヒューマンインターフェイス部をもさらに

具備してなるICカードの構成採用にある。

【0033】本発明カードの第14の特徴は、上記本発明カードの第13の特徴におけるヒューマンインターフェイス部が、人手入力自在な入力部を具备してなるICカードの構成採用にある。

【0034】本発明カードの第15の特徴は、上記本発明カードの第13の特徴におけるヒューマンインターフェイス部が、外部認識自在な出力部を具备してなるICカードの構成採用にある。

10 【0035】本発明カードの第16の特徴は、上記本発明カードの第13の特徴におけるヒューマンインターフェイス部が、前記入力部と前記出力部を併せて具备してなるICカードの構成採用にある。

【0036】本発明カードの第17の特徴は、上記本発明カードの第14又は第16の特徴における入力部が、受益サービス選択機能を有してなるICカードの構成採用にある。

20 【0037】本発明カードの第18の特徴は、上記本発明カードの第14、第16又は第17の特徴における入力部が、手書き入力手段であるICカードの構成採用にある。

【0038】本発明カードの第19の特徴は、上記本発明カードの第18の特徴における手書き入力手段が、入力された情報を解読しコード化する手書き入力認識機能を具备してなるICカードの構成採用にある。

【0039】本発明カードの第20の特徴は、上記本発明カードの第19の特徴における入力が、文字入力、図形入力若しくは絵入力又はそれらの組合せであるICカードの構成採用にある。

30 【0040】本発明カードの第21の特徴は、上記本発明カードの第14又は第16の特徴における入力部が、音入力手段であるICカードの構成採用にある。

【0041】本発明カードの第22の特徴は、上記本発明カードの第21の特徴における音入力手段が、入力された音を解読しコード化する音声認識機能を有してなるICカードの構成採用にある。

【0042】本発明カードの第23の特徴は、上記本発明カードの第15又は第16の特徴における出力部が、表示手段、LEDランプ若しくは音出力手段又はこれらの組合せ手段であるICカードの構成採用にある。

【0043】本発明カードの第24の特徴は、上記本発明カードの第23の特徴における音出力手段が、コード化されたコードデータを音出力する音合成機能を有してなるICカードの構成採用にある。

【0044】本発明カードの第25の特徴は、上記本発明カードの第16の特徴における入力部と出力部が、一体化された音声入出力手段であるICカードの構成採用にある。

50 【0045】本発明カードの第26の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7、第

8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18、第19、第20、第21、第22、第23、第24又は第25の特徴におけるデータ入出力部が、ICカードに対応する端末との通信の為の無線通信機能を具備してなるICカードの構成採用にある。

【0046】本発明カードの第27の特徴は、上記本発明カードの第26の特徴における無線通信機能が、ISO10536、ISO14443、ISO15693、PHS方式、IMT2000に準拠してなるICカードの構成採用にある。

【0047】本発明カードの第28の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18、第19、第20、第21、第22、第23、第24、第25、第26又は第27の特徴におけるデータ入出力部が、暗号化されたデータを入出力自在としてなるICカードの構成採用にある。

【0048】本発明カードの第29の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18、第19、第20、第21、第22、第23、第24、第25、第26、第27又は第28におけるICカードが、電源のON/OFFを制御可能とするスイッチ手段を具備してなるICカードの構成採用にある。

【0049】本発明カードの第30の特徴は、上記本発明カードの第29の特徴におけるスイッチ手段が、ICカード外部からの信号を受信し、電源供給をON状態にする機能を有してなるICカードの構成採用にある。

【0050】本発明カードの第31の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18、第19、第20、第21、第22、第23、第24、第25、第26、第27、第28、第29又は第30の特徴における認証用センサー部が、指紋読み取りセンサー、手書き読み取りセンサー、音声センサー若しくは虹彩読み取りセンサー、又は前記センサーを組み合わせた複合センサーであるICカードの構成採用にある。

【0051】本発明カードの第32の特徴は、上記本発明カードの第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18、第19、第20、第21、第22、第23、第24、第25、第26、第27、第28、第29、第30又は第31の特徴における認証用センサー部が、ICカードを保持した際に自動的に認証を実行自在な配置としてなるICカードの構成採用にある。

【0052】本発明カードの第33の特徴は、上記本発明カードの第32の特徴における配置が、ICカードの保持する指接触にて自発的に指紋認証処置を実行せしめるよう、当該ICカードの表面の大部分を指紋センサーにて占有せしめてなる、ICカードの構成採用にある。

【0053】本発明使用方法の第1の特徴は、上記本発明のICカードと、当該ICカードを処理可能な端末及び当該端末に接続可能なサービスセンタとからなるICカードサービス利用システム装置の利用に当たり、最初10だけ、前記サービスセンタに前記ICカードを前記端末を介し接続して個人IDの新規登録を行ってから、ICカード及びサービスセンタ相互間の利用環境設定をその都度行うことにより、所望のサービスを当該ICカードと当該サービスセンタ間で要求提供してなるICカード使用方法の構成採用にある。

【0054】本発明使用方法の第2の特徴は、上記本発明使用方法の第1の特徴における新規登録が、ICカードによる個人認証の結果を考慮して行い、端末からサービスセンタに送信された個人IDに基づき事前に届けられた使用不可の個人IDに該当するかどうかの当該サービスセンタでの利用可能性を判断した結果に基づき、利用可能の場合には、サービスセンタに個人IDの登録を行い、端末は当該サービスセンタから送信されたサービスIDをICカードに送信し、ICカードの不揮発性メモリに当該サービスIDを記憶する、以上一連のステップを踏んで実行されてなるICカード使用方法の構成採用にある。

【0055】本発明使用方法の第3の特徴は、上記本発明使用方法の第1又は2における利用環境設定が、IC30カードによる個人認証の結果を考慮して行い、サービス受益者が端末又は前記ICカードに対してサービス使用権情報に関する設定後、当該設定されたサービス利用環境を個人IDと共にサービスセンタに送信し、当該サービスセンタは送信された情報を確認した後に当該サービスセンタ内に記憶させ、端末又はICカードは、当該ICカードの不揮発性メモリにサービスセンタに記憶させた情報と同一の情報を書き込み登録させる、以上一連のステップを踏んで実行されてなるICカード使用方法の構成採用にある。

【0056】本発明使用方法の第4の特徴は、上記本発明使用方法の第3の特徴における端末が、サービス要求者からの個人IDの投入があると、当該サービス要求者に対して個人認証必要性をサービス使用権情報から判定し、当該判定の結果必要な場合のみ、ICカード内の認証用センサ部によりある固有の身体的特徴抽出処理を行った後、処理結果を前記個人認証用データと照合することにより個人認証判定を行い、当該個人認証判定が不要又は正の場合には、サービスセンタに端末から前記個人ID及びサービスIDを送信し、当該サービスセンタ50は送信情報を確認後、サービス提供可能と判断した場合

には要求されたサービスを提供する、以上一連のステップを踏んで処理してなるICカード使用方法の構成採用にある。

【0057】本発明使用方法の第5の特徴は、上記本発明使用方法の第3の特徴におけるICカードが、端末よりサービスIDを受信すると、個人認証必要性をサービス使用権情報から判定し、当該判定の結果必要な場合のみ、認証用センサ部によりある固有の身体的特徴検出処理を行った後、当該処理結果を前記個人認証用データと照合させることにより個人認証判定を行い、当該個人認証判定が不要又は正の場合には、サービス利用環境の設定からサービスの提供か否かを判断し、サービス提供可能と判断された場合には、サービス提供を行う、以上一連のステップを踏んで処理してなるICカード使用方法の構成採用にある。

【0058】本発明使用方法の第6の特徴は、上記本発明使用方法の第4又は第5の特徴におけるサービス提供可能との判断が、ICカード内の不揮発性メモリ及びサービスセンタにサービス提供実施に関するサービス提供情報の追加記憶を実行させてなるICカード使用方法の構成採用にある。

【0059】本発明使用方法の第7の特徴は、上記本願発明使用方法の第6特徴におけるサービス提供情報が、端末を介して当該端末とサービスセンタとがサービスID又は個人IDを送受信する際に同時に送信され、当該サービス提供情報に関わる送信された情報と自己が記憶している情報とが合致する否かを確認され、不一致の場合には、サービス提供を中止させる、以上一連のステップを踏んで実行させてなるICカード使用方法の構成採用にある。

#### 【0060】

【発明の実施の形態】以下、添付図面を参照しながら、本発明の実施の形態につきそのカード例及び方法例を説明する。

【0061】(カード例1)図1は、本ICカードのカード例1の構成を示したものである。ICカードAは、認証用センサ一部1、データ処理部2、不揮発性メモリ3、電源供給を受けるための電源供給用端子又は電源供給部を有する電源関係部4、主記憶部5、書換不可能なメモリ6、データ入出力部7から構成される。

【0062】前記認証用センサ一部1は、指紋の身体的特徴を読み取るためのものである。前記書換不可能なメモリ6は、個人認証用データ、個人ID、カードID等を個別に保持するためのものである。これら個人に関する情報は書換不可能なメモリ6に保持されることにより、個人情報の改竄を防止することができる。ここで、書換不可能なメモリ6は、形態上書換が不可能なメモリー例えはROMのみならず、保存されているデータにプロテクトをかけて当該プロテクトを除去しなければ書き換えができない等の書き換え不可能な論理構造としたメモリ

でもよい。

【0063】不揮発性メモリ3は、サービス利用権情報、即ち、サービスIDの他に、サービス受益期間、サービス受益回数その他のサービス提供条件及びある固有の身体的特徴検出処理の要否情報を記憶させ、追加書き込みができるものである。一のICカードAで複数のサービスを要求できる場合には不揮発性メモリ3には各サービス毎に各サービス利用権情報が記憶されることになる。

10 【0064】なお、主記憶部5は主として本ICカードAのプログラム等の制御内容を記憶させるためのものであり、データ処理部2は主記憶部5から適宜ICカードA内の各部から、認証センサ一部1によるセンサの読み取り情報、書換不可能なメモリ6から個人認証用データ等、不揮発性メモリ3からサービス利用権等情報を検索読み出すほか、認証の一一致不一致の判断、不揮発性メモリ3に各情報を読み記憶させる等の本ICカードA内の制御を実際に行うMPU部分である。

【0065】ICカードAにおいては、指紋センサーによる指紋認証を挙げたが、これに限ることなく、手書き文字入力パレットを装備した手書き文字による認証、音声入力装置を備えた音声認証、虹彩読み取り装置を備えた虹彩認証、その他の認証でも良いことは言うまでもない。

【0066】また、必要に応じて、不正使用を防止するセキュリティを有するICカードAとして、不揮発性メモリ3において、過去の書き込み情報を消去せずに保持する機能を備え、過去のサービス情報履歴を読み出し、ICカードA内サービス情報履歴とカード外、例えばサードパーティ内のサービス利用履歴と照合させることにより、不正使用の判断が可能となる。

【0067】実際には、ICカードAは認証結果やサービス情報をデータ入出力部7により他の連携機器と通信して初めて使用可能となるが、この通信を、従来の接触式で行うと、ICカードAを、例えばリードライターに挿入することが必要となり、挿入ミス等により再度挿入しなければならず手間がかかるばかりか、延いては、ICカードAを破損する虞がある。その為に、データ入出力部7において無線通信機能を具備し非接触式で行うと良い。

【0068】無線通信の実現手段としては、ISO10536規格、ISO14443規格、ISO15693規格又は従来携帯データ端末で使用されている、PHS方式、IMT2000等の一般に認知されている方式を用いることにより、ICカードAの利用領域が一段と拡大し、これによりユーザの利用し易いICカードAを提供できる。

【0069】ここで、上記の各種通信手段により、ICカードA内に格納されている個人情報の通信が行われるが、通信中の情報の漏洩を防止する為に、その手段とし

て、情報の暗号化が極めて有効であり、ICカードA内に情報の暗号化及び暗号情報の解読の機能を付加することにより、ICカードAの不正な使用を防止するとは別の意味におけるセキュリティの高いICカードAを提供できる。

【0070】以上、カード例1について説明したが、カード例1を基本構成として下記する他のカード例の様に応用的な構成手段を具え、適宜変更することができる。

【0071】(カード例2)図2は本カード例2の構成を示したものである。ICカードBは、図1に示す前記カード例1のICカードAに出力部8を追加したものである。ここで、出力部8は、液晶表示装置を内蔵させて文字、図、絵等を表示したり、LEDランプを内蔵して光を点灯又は点滅させたり、スピーカを内蔵して音を発生させる等適宜ICカードの使用形態に応じて選択することができる。

【0072】この構成により、例えば、認証用センサー部1からの読み取り情報とICカード内の個人認証用データとを照合させた結果をその場において表示、光や音により確認することや、出力部8に表示機能を持たせた場合には出力部8にサービスメニューを表示することが可能となり、ヒューマンインターフェース機能が向上したICカードBの提供が可能となる。

【0073】(カード例3)図3は、本カード例3の構成を示したものである。ICカードCは、図2に示す前記カード例2のICカードBに、受益サービス選択部9を追加したものである。ICカード自体が多機能となるに従い、機能の選択、設定等が複雑となるが、これを受益サービス選択部9により、従来必要であった他の連携機器における設定処理が不要となり、ICカードCの操作のみにより機能の選択、設定を行うことが可能となる。

【0074】また、出力部8に機能選択、設定等の操作結果を表示し、確認することが可能となる。受益サービス選択部9としては、例えば出力部8に表示機能を備えた表示装置内のカーソルを移動させるためのスイッチパットが挙げられる。

【0075】具体的には、ICカードCが定期券の場合、回数券の場合の何れかの場合として使用するのではなく、一のICカードにより定期券、回数券両方の機能を備えても良い。なお、ICカードCは出力部8を備えているが、必ず必要というものではない。

【0076】(カード例4)図4は、本カード例4の構成を示したものである。ICカードDは、図1に示す前記カード例1のICカードAに、音声出力部10及び音声入力部11を追加したものである。音声出力部10及び音声入力部11は音声により機能の選択、設定等を可能せしめるヒューマンインターフェースである。

【0077】これにより、機能に対応したキーワードを音声により入力することができる。これにより、音声と

いう極めて人間に優しいヒューマンインターフェースにてICカードDと対話でき、面倒な受益サービス選択部9を操作する必要がなく、非常に使用し易いICカードDを提供することができる。

【0078】この場合、音声認識、音声合成を行う必要がある。これらを実行する方法として、データ入出力部7の通信を介して他の連携機器にて行う形式とICカードD内にて行う形式とが考えられる。

【0079】ICカードD内の、例えば、データ処理部10又は音声出力部10及び音声入力部11にて、音声認識及び音声合成を行う方が通信処理不要のため高速処理が可能となり非常に使い勝手の良いヒューマンインターフェースを具えたICカードDを提供できる。また、音声出力部10と音声入力部11とは音声入出力部として一体構成させて、音声認識、音声合成を行っても良い。

【0080】(カード例5)図5は本カード例5の構成図を示したものである。ICカードEは、図1に示す前記カード例1のICカードAに手書き入力部12を追加したものである。手書き入力部12としては、例えば液晶タブレットが挙げられる。手書き入力部12の実際の大きさは入力を受付ける内容に応じて決めれば良い。

【0081】これにより、手書き入力により機能の選択設定等が行えるヒューマンインターフェイスを具えたICカードEを提供することができる。手書き入力部12には、文字のみならず図形、絵等も入力することができる。これにより、手書き入力という人間に優しいヒューマンインターフェイスでICカードEと対話可能となり、面倒な受益サービス選択部9を操作する必要がなくなる。よって、非常に使用し易いICカードEを提供できる。

【0082】ここでは、手書き入力による機能の選択設定等の作業を挙げているが、例えば目的とするサービスを自動的に検索可能とするように、ICカードE内に保持された情報の検索機能を備えることにより、機能の選択設定等を容易に行え更に使い勝手の良いICカードEを提供することができる。

【0083】この処理を実行する方法として、データ入出力部7の通信を介して他の連携機器にて行う方法とICカードEのデータ処理部2にて行う方法とが考えられるが、ICカードEのデータ処理部2で行う方が通信による処理が不要のため高速処理が可能となり非常に使い勝手の良いヒューマンインターフェースを提供できる。

【0084】つまり、データ入出力部7を通じサービスを要求する端末にICカードEを近づけることにより、端末から出力されたセンサー情報をICカードEが入力し、当該センサーの情報に基づき、データ処理部2により、機能を選択することができる。

【0085】このように、サービス要求を受付ける手段そのものが、そのサービス内容に関する情報を発信し、50それを感知したICカードEは、サービス内容に関する

情報から、一のICカードEに予め設定されたサービスIDを特定し、そのサービスIDに対するサービス条件や個人認証の要否をICカードE内で確認判断することができる。この点は図1～図4に示す他のカード例1～4においてもいえることである。

【0086】(カード例6)図6は本カード例6の構成を示したものである。ICカードFは、図1に示す前記カード例1のICカードAに電源スイッチ13を追加したものである。ICカードF自体はその場その場で瞬時な処理を行うために絶えず電源状態がONである方が良いが、電源スイッチ13を設けることにより、絶対に使用しない時に電源状態をOFFにできる。これにより電力消費を節約することができる。

【0087】(カード例7)図7は本カード例7の構成を示したものである。ICカードGは、図1に示す前記カード例1のICカードAに電源スイッチ信号発生部14を追加したものである。わざわざ電源スイッチ13を操作する必要をなくすために、電源スイッチ13の代わりに、電源スイッチ信号発生部14を設けたものである。例えば、一定時間ICカードGの何等かの動作がなければ電源スイッチを自動的にOFFにしておき、他の連携機器からの信号を受信すると、電源スイッチ信号発生部14が作動し電源スイッチがONとなるようにすることにより、わざわざ電源スイッチ13を操作しなくても電力消費を節約することができるという利点がある。

【0088】(カード例8)図8は本カード例8の構成を示したものである。ICカードHは、図1に示す前記カード例1のICカードAと比較すると、認証用センサー部1の位置及び当該ICカードHに占める表面積の割合が異なる。即ち、ICカードHは、個人の特徴を抽出するセンサー部が指紋センサーであり、ICカードHを自然に手で持った際触れた指にて指認証処理を行えるように、指紋センサーを習性的に把持傾向にある部域に亘り配設したICカードHである。

【0089】前記ICカードAでは、指紋センサー1の定位置を使用者が認識し指を当てる行為をする必要があるが、ICカードHでは認証用センサー1が占める表面積の割合を大きく、かつ図8に示したように人間の特性に注目してICカードHを使用する際に習性的に指で触る頻度の高い部分に、指紋センサー1を配置することにより、使用者がICカードHを持った時点で自動的に指紋認証処理を実行することができ、極めて使いやすいICカードHを提供することができる。

【0090】以上、ICカードとして、その基本構成としてカード例1を説明し、更なる利便性を向上させるべくカード例2乃至8を説明したが、それぞれの構成の利点を複合させて、それぞれの利点を持たせることができ、そのための機能モジュールを複数有するICカードにすることにより、より使い勝手の良いICカードが提供できる。

【0091】(セキュリティレベル設定判定方法例)次に、前記カード例1～8に適用するセキュリティレベル設定判別方法例の処理手順を説明する。

【0092】ICカードA～Hの不揮発性メモリ3にサービス内容に応じたサービス利用権情報を記憶させることにより、当該サービス使用権情報に基づきサービス提供時における認証用センサー部1による個人認証必要性の有無を任意に設定可能であり、様々なサービスセキュリティレベルの設定が可能となり、よってサービスプロバイダーからの要求に応えることが可能となる。そして、サービスを要求する際に、ICカードA～Hの不揮発性メモリ3の記憶状態から、個人認証の必要性の有無を判別する。

【0093】例えば、ICカードA～Hを定期券、回数券として利用する場合、それぞれ、定期利用期間、利用回数がサービス使用権情報のサービス提供条件として不揮発性メモリ3に記憶される。これにより、サービス使用権情報として、ICカードA～Hでの個人認証処理を行うことなく、サービスの受益の、期限的な、回数的な制約を加えることが可能となる。定期券としてICカードA～Hを利用する場合、受益期間中個人認証を不要として設定可能であり、面倒な処理が不要となる。

【0094】また、回数券としてICカードA～Hを利用する場合、個人認証が不必要的回数を同時に改札機にて確認でき、ICカードA～H内に保持されている利用回数を減じればよい。回数券の場合においても使用期限があるような場合には、サービス受益期間も設定することにより対処可能となる。また、サービス提供条件が特に無く、個人認証の必要性の有無だけを設定することが可能である。具体的には、以下に説明するICカードシステムにICカードA～Hの使用方法の実施例にて説明する。

#### 【0095】

【実施例】カード例のICカード使用方法例の実施手順を説明する。前記本使用方法例の説明に先立って、本使用方法例が利用するICカードサービス利用システム $\alpha$ を図9について説明する。ICカードサービス利用システム $\alpha$ は、前記カード例1～8のセキュリティレベル設定判別可能なICカードA～Hと、当該ICカードA～Hを処理可能な端末 $\beta$ と、サービスセンタ(サーバ) $\gamma$ とを有する。

【0096】サービスセンタ $\gamma$ と端末 $\beta$ は専用回線、ネットワーク回線若しくはそれらの結合された通信網等の通信回線 $\delta$ で接続され、一方、セキュリティレベル設定判別可能なICカードA～Hと端末 $\beta$ は有線、無線何れによる接続であっても良い。

【0097】上記はシステム $\alpha$ の基本構成であり、適宜必要に応じて各種の装置を追加、又は当該基本構成と同様の動作をする装置に変更可能である。例えば、端末 $\beta$ は当該ICカードA～Hと情報のやり取りを行えるもの

19

であればコンピュータ等の情報通信機器でも良い。サービスセンタ $\gamma$ は複数当該通信回線 $\delta$ に接続され、複数のサービスを提供できるものである方がよいが、一のサービスでも良い。

【0098】ICカードサービス利用システム $\alpha$ の利用によりICカードA～Hを使用して端末 $\beta$ を通しサービスを要求する際、予め受けたいサービスに対して、当該サービス提供者であるサービスセンタ $\gamma$ とコンタクトして新規登録し、ICカードA～H及び当該サービスセンタ $\gamma$ に利用環境設定を相互間で行う必要性がある。なお、以下の説明において、回線 $\delta$ 接続等の通常必要となる操作については省略して、本発明の根幹に関わる部分のみを説明する。

【0099】<新規登録>図10は、ICカードA～Hと連携した端末 $\beta$ でサービスセンタ $\gamma$ に対してネットワークサービスを受けるための新規登録の際のICカードサービス利用システム $\alpha$ の利用ステップを示したものである。

【0100】先ず、端末 $\beta$ からユーザ個人に対して個人IDの要求がなされる(ST1)。投入後、ICカードA～Hにて個人認証が行われ(ST2)、個人認証の結果(ST3)、既に登録されている個人情報と一致すれば、サービスセンタ $\gamma$ に個人IDが送信され(ST4)、不一致であれば、ユーザに対して登録不可通知が提示される(ST5)。なお、ST2は必要に応じて省略可能であり、その場合にはST4へ進むことになる。

【0101】ST4の後、サービスセンタ $\gamma$ 内のサーバにおいて個人IDがチェックされる(ST6)。ここでの個人IDのチェックとは、例えば、ICカードA～H内の書換不可能なメモリ6に記憶されている個人IDがそのサービスセンタ $\gamma$ の規定に当てはまっているかどうかとか、各サービスセンタ $\gamma$ 間でのサービスを提供しないように予め個人IDをリストとして保有しておりそのリスト中に該当するかどうかとか、サービス提供開始前にサービスをカード保持者が要求してきた際にサービスを提供しないようにする等の、サービスセンタ $\gamma$ がサービスを提供しても良いかどうかを個人IDに基いてチェックする。

【0102】そして、利用可能か否かが判定される(ST7)。この際、サービス利用が不可であればユーザに対して登録不可通知が提示され(ST5)、利用可能であれば、サービスセンタ $\gamma$ 内のサーバにおいて新規サービスに対する個人IDをサービスセンタ $\gamma$ に登録し(ST8)、ユーザに登録完了を通知し(ST9)、ICカードの不揮発性メモリ3にサービスIDを記録登録する(ST10)。

【0103】<サービス利用環境の設定>図11は、ユーザが新規登録済みのICカードA～Hにサービス利用環境を設定して設定情報をサービスセンタ $\gamma$ に通知後、ICカードA～Hに当該設定情報を書き込むという、サ

20

ービス利用環境の設定の際のICカードサービス利用システム $\alpha$ の実行進歩ステップの動作を示したものである。

【0104】先ず、端末 $\beta$ からユーザに対して、個人IDの要求がなされる(S1)。投入後、ICカードA～Hにて個人認証が行われる(S2)。個人認証の判定(S3)により、既に登録済みの個人情報と一致しない場合にはユーザに対して登録不可通知を提示し(S4)、一致する場合には端末 $\beta$ にてサービス利用環境設定を行なう(S5)。

【0105】当該サービス利用環境の設定として、セキュリティレベル設定判定方法例として前記したように、例えばICカードA～Hでの個人認証が不要なサービス受益期間や回数を設定することができる。その後、サービスセンタに個人ID及び設定したサービス利用環境を送信する(S6)。

【0106】サービスセンタ $\gamma$ 内のサーバでは、送信されたサービス利用環境を確認する(S7)。確認判定(S8)により、不適切であればユーザへ登録不可通知を提示し(S4)、適切であればサービス利用環境の設定登録を行い(S9)、ユーザに登録完了を通知し(ST10)、ICカードの不揮発性メモリ3にサービス利用環境データを書き込み登録する(ST11)。

【0107】(実用例)以上の設定を行なったのちの実行手順の実用例を以下に示すが、ここでは、サービスとして定期刊行物電子配信サービス及び電子改札券サービスを挙げ、サービス提供条件が受益回数、受益期間のそれぞれについて順に説明していく。

【0108】<定期刊行物電子配信サービスの場合>図30 12、図13は、ICカードによる定期刊行物電子配信サービスを想定した際のICカードサービス利用システム $\alpha$ の実行手順を示したものであり、サービス提示条件が図12では受益期間の場合、図13では受益回数の場合である。

【0109】図12のサービス提供条件が受益期間の場合について説明する。先ず、端末 $\beta$ から個人に対して個人IDの要求がなされる(SE1)。投入すると、ICカードA～Hによる個人認証の要否の確認がなされる(SE2)。ここで、個人認証不必要サービス受益期間外であり個人認証が必要と判断されると、個人認証が行われ(SE3)、その結果が既に登録済みの個人情報と一致不一致の判定がなされる(SE4)。

【0110】不一致の場合にはユーザに電子配信不可の通知を行い(SE5)、一致した場合にはサービスセンタ $\gamma$ のサーバに対し、個人ID及びサービスIDが送信される(SE6)。一方、SE2にて不要であると判断された場合には、サービスセンタ $\gamma$ 内のサーバに対し、個人ID及びサービスIDが送信される(SE6)。

【0111】サービスセンタ $\gamma$ 内のサーバにおいて、受50 信した個人ID及びサービスIDを確認する(SE

7)。ここで、確認判定(SE8)の結果、利用不可であればユーザに対し電子配信不可を通知し(SE5)、利用可能であればユーザに対して定期刊行物電子配信がサービスセンタから端末βに対して行われる(SE9)。電子配信終了後、ユーザはサービスセンタのサーバに対して電子配信完了を通知する(SE10)。これにより一連の動作が終了する。

【0112】次に、図13のサービス提供条件が受益回数の場合を説明する。先ず、端末βから個人に対して個人IDの要求がなされる(SE1)。投入すると、ICカードA~Hによる個人認証の要否の確認がなされる(SE2)。ここで、個人認証不必要サービス回数外であり個人認証が必要と判断されると、個人認証が行われ(SE3)、その結果が既に登録済みの個人情報と一致不一致の判定がなされる(SE4)。

【0113】不一致の場合ユーザにサービス利用不可の通知を行い(SE5)、一致した場合サービスセンタ内のサーバに対し、個人ID及びサービスIDが送信される(SE6)。一方、SE2にて個人認証不必要回数内であり個人認証不要であると判断された場合には、サービスセンタ内のサーバに対し、個人ID及びサービスIDが送信される(SE6)。

【0114】サービスセンタ内のサーバにおいて、受信した個人ID及びサービスIDを確認する(SE7)。ここで、確認判定(SE8)の結果、利用不可であればユーザに対し電子配信不可を通知し(SE5)、利用可能であればユーザに対して定期刊行物電子配信がサービスセンタから端末βに対して行われる(SE9)。電子配信終了後、ICカードA~H内の不揮発性メモリ3内の受益回数データを一減算する処理を行う(SE11)。そして、端末β側の処理において、ユーザからのサービスセンタへ配信完了を通知する(SE12)。そして一連の実行が終了する。

【0115】何れの場合においても、サービスセンタがサービスの提供を行った際に、個人ID、サービスID、実際に受益した回数、その他のサービスの提供に関する情報を電子配信の際同時に端末βに送信し、その情報をICカードA~H内の不揮発性メモリ3に追加書き込みを行うと共に、当該サービスセンタ内のサーバにも記憶させておく。

【0116】そして、次回サービス提供の要求がなされた場合に、端末βからサービスセンタに個人ID、サービスIDを送信する(SE6の)際に、同時に不揮発性メモリ3内に追加書きした情報も同時に送信し、サービスセンタでの個人ID、サービスIDの確認(SE7)の際、同時にICカードA~Hに追加書き込みされていた情報と、サービスセンタ内に追加書き込みした情報とが同一であるか否かを判断することにより、不正な取り引きをなくすことができる。

【0117】これにより、定期刊行物電子配信の様な電

子商品取引において、所定の規定を有した基準を個々のサービスに対して定めることにより、電子商品取引において不正な取り引きを防止し、円滑な経済、商業活動が行われる。

【0118】<電子改札券サービスの場合>図14、図15に電子改札券サービスを想定した際のICカードサービス利用システムαの利用を示したものである。図14はサービス受益期間が設定された場合、具体的には定期券の場合、図15はサービス受益回数が設定された場合、具体的には期限無しの回数券の場合である。

【0119】サービス受益期間が設定された場合について、図14を参照しながら説明する。先ず、改札ゲートから個人のICカードA~Hに対してサービスIDが送信される(SG1)。すると、当該サービスの個人認証の要否がICカードA~H内の不揮発性メモリ3のサービス使用権情報により確認される(SG2)。

【0120】個人認証が必要と判断された場合には個人認証が行われ(SG3)、認証結果の判定がなされる(SG4)。そして、偽であると判定された場合には、改札ゲートは閉鎖状態となる(SG5)。一方、正であると判定された場合には、ICカードA~H内でサービス受益期間の照合がなされ(SG6)、サービス受益期間対象内である場合、改札ゲートに対して通過依頼を要求し(SG7)、改札ゲートは開放状態となる(SG8)。サービス受益期間対象外である場合、改札ゲートは閉鎖状態となる(SG5)。

【0121】個人認証が不要であると判断された場合、ICカードA~H内でサービス受益期間の照合がなされる(SG6)。サービス受益期間対象内と判断されたら、改札ゲートに対して通過依頼を要求し(SG7)、改札ゲートは開放状態となる(SG8)。サービス受益期間対象外と判断されたら、改札ゲートは閉鎖状態となる(SG5)。

【0122】サービス受益回数が設定された場合について、図15を参照しながら説明する。先ず、改札ゲートから個人のICカードA~Hに対してサービスIDが送信される(SG1)。すると、当該サービスの個人認証の要否がICカードA~H内の不揮発性メモリ3のサービス使用権情報により確認される(SG2)。

【0123】個人認証が必要とされた場合には、個人認証が行われ(SG3)、認証結果の判定がなされる(SG4)。そして、偽であると判定されたら、改札ゲートは閉鎖状態となる(SG5)。正と判定されたら、ICカードA~H内でサービス受益期間の照合がなされ(SG6)、サービス受益回数内である場合、改札ゲートに対して通過を依頼し(SG7)、改札ゲートは開放状態となり(SG8)、ICカードA~H内の不揮発性メモリ3内の受益回数減算処理を行う(SG9)。サービス受益期間対象外である場合、改札ゲートは閉鎖状態となる(SG5)。

【0124】個人認証が不要とされた場合には、ICカードA～H内でサービス受益期間の照合なされる(SG6)。そして、サービス受益期間対象内である場合、改札ゲートに対して通過を依頼し(SG7)、改札ゲートは開放状態となり(SG8)、ICカードA～H内の不揮発性メモリー内の受益回数減算処理を行う(SG9)。一方、サービス受益期間対象外である場合、改札ゲートは閉鎖状態となる(SG5)。

【0125】定期刊行物電子配信サービスの場合と同様に電子改札券の場合においても、個人ID、サービスID、実際に受益した回数、その他のサービスの提供に関する情報を、改札ゲート内の記憶装置に追加書き込みできる様にすることにより不正なサービス要求に対する防止が可能となる。

【0126】つまり、認証不要と判断した場合には認証要否の判定(SG2)後、認証必要と判断した場合には個人認証判定(SG4)後に、電子改札券内の追加書き込み情報の過去の履歴を改札ゲートに送信し、送信された情報と、改札ゲート内の記憶装置内に追加書き込みされた情報と一致するかどうかを確認することにより、不正なサービス要求に対処できる。

【0127】また、必ずしも改札ゲート内に追加書き込みできる記憶装置を設ける必要はなく、幾つもの改札ゲートと接続したセンタに個人情報、追加書き込む情報を記憶させて不正なサービス要求の防止を行うことができる。

【0128】さらに、逐一不正なサービス要求防止のための確認を行うと確認する情報が膨大となる場合があるので、通常は前回のサービス要求提供の際に改札ゲートとICカードA～Hとのやり取りを行ったデータのみが一致するか否か確認し、必要に応じて過去履歴を確認する等のサービスの内容、セキュリティレベルに応じて適宜変更を加えることにより、敏速なサービス要求提供の作業がなされる。

#### 【0129】

【発明の効果】以上説明したように、本発明によれば、高いセキュリティが必要なサービス、それほど高くないサービス等のようにセキュリティレベルの異なるサービスに対して、柔軟に個人認識の処理の有無を設定でき、極めて利便性の高いICカード、ICカード使用方法、セキュリティレベル設定判別方法を提供することができる。また、ヒューマンインターフェイスを具えたICカード、ICカードサービス利用システムを同時に提供することができる。更に、不正使用に対して極めて耐性の高いICカード、ICカード使用方法、セキュリティレベル設定方法を提供することができる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態を示すICカードの基本構成であるカード例1の内部構成ブロック図である。

【図2】同上カード例1に出力部を追加したカード例2

の内部構成ブロック図である。

【図3】同上カード例2に受益サービス選択部を追加したカード例3の内部構成ブロック図である。

【図4】同上カード例1に音声入力部、音声出力部を追加したカード例4の内部構成ブロック図である。

【図5】同上カード例1に手書き入力部を追加したカード例5の内部構成ブロック図である。

【図6】同上カード例1に電源スイッチを追加したカード例6の内部構成ブロック図である。

【図7】カード例1に電源スイッチ信号発生部を追加したカード例7の内部構成ブロック図である。

【図8】本発明の実施の形態を示すカード例8の内部構成ブロック図である。

【図9】本発明の実施の形態の実施例を示すICカード使用方法例が利用するICカードサービス利用システムの模式図である。

【図10】同上使用方法例における新規登録の際のICカードサービス利用システムの利用を示したフローチャートである。

【図11】同上使用方法例を示すサービス利用環境設定の際のICカードサービス利用システムの利用を示したフローチャートである。

【図12】同上実用例を示す定期刊行物電子配信サービスの受益期間を想定した場合のICカードサービス利用システムの利用を示したフローチャートである。

【図13】同上の実用例に示す定期刊行物電子配信サービスの受益回数を想定した場合のICカードサービス利用システムの利用を示したフローチャートである。

【図14】同上の他の実用例を示す電子改札券サービスシステムの受益期間を想定した場合のICカードサービス利用システムの利用を示したフローチャートである。

【図15】同上の他の実用例を示す電子改札券サービスシステムの回数券を想定した場合のICカードサービス利用システムの利用を示したフローチャートである。

#### 【符号の説明】

1…認証用センサー部

2…データ処理部

3…不揮発性メモリ

4…電源関係部

5…主記憶部

6…書換不可能なメモリ

7…データ入出力部

8…出力部

9…受益サービス選択部

10…音声出力部

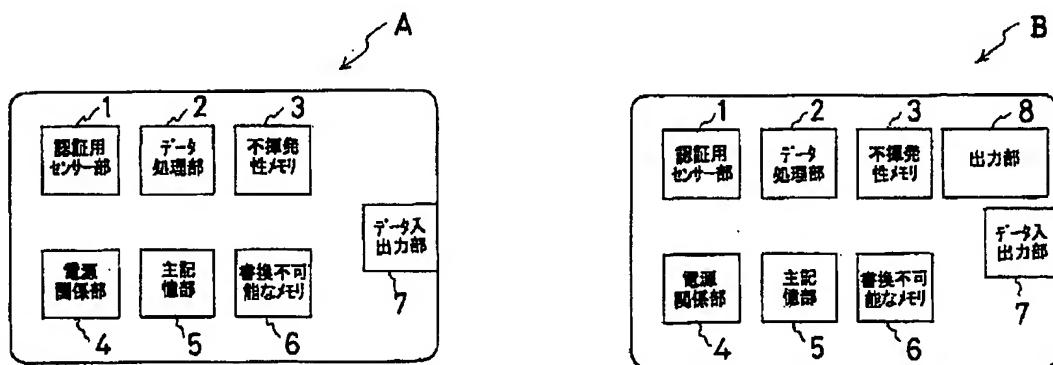
11…音声入力部

12…手書き入力部

13…電源スイッチ

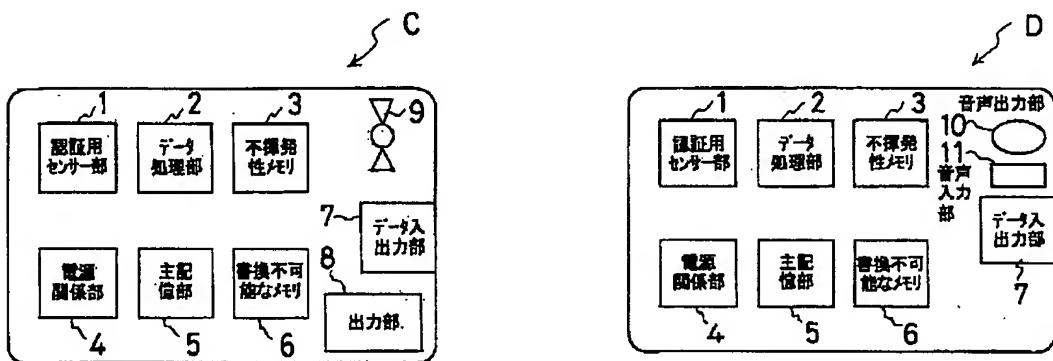
14…電源スイッチ信号発生部

50 A, B, C, D, E, F, G, H…ICカード



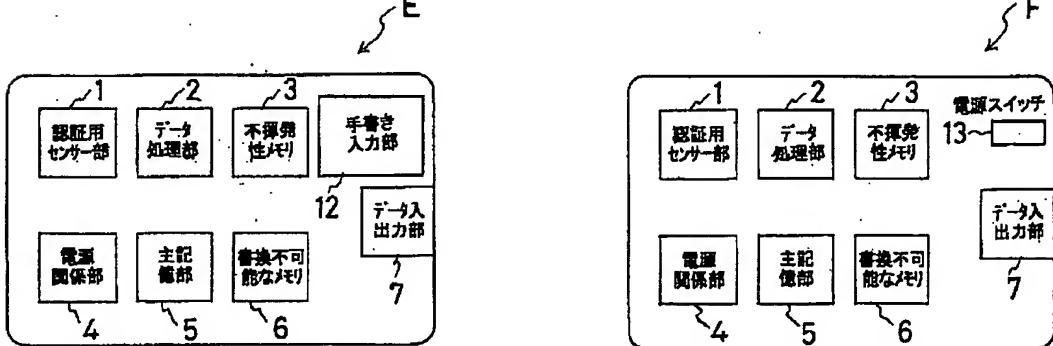
【図3】

【図4】

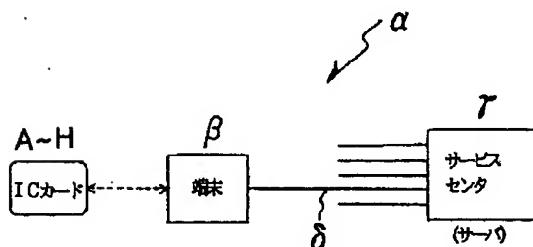


【図5】

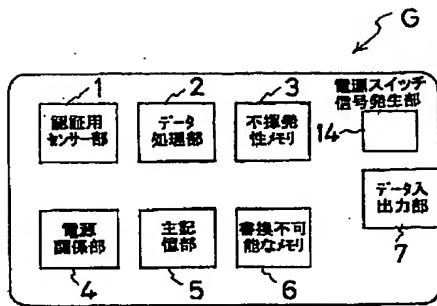
【図6】



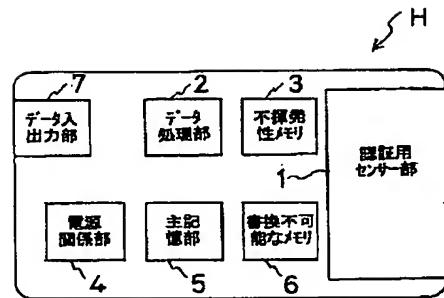
【図9】



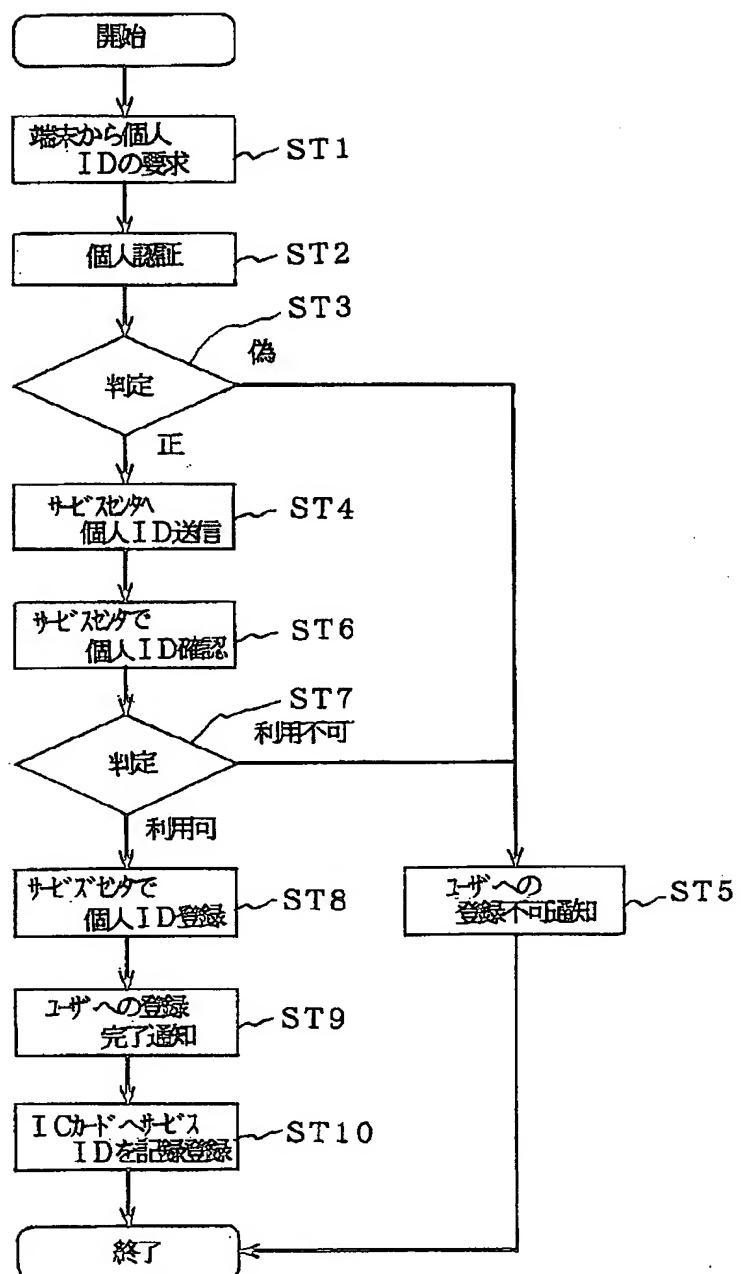
【図7】



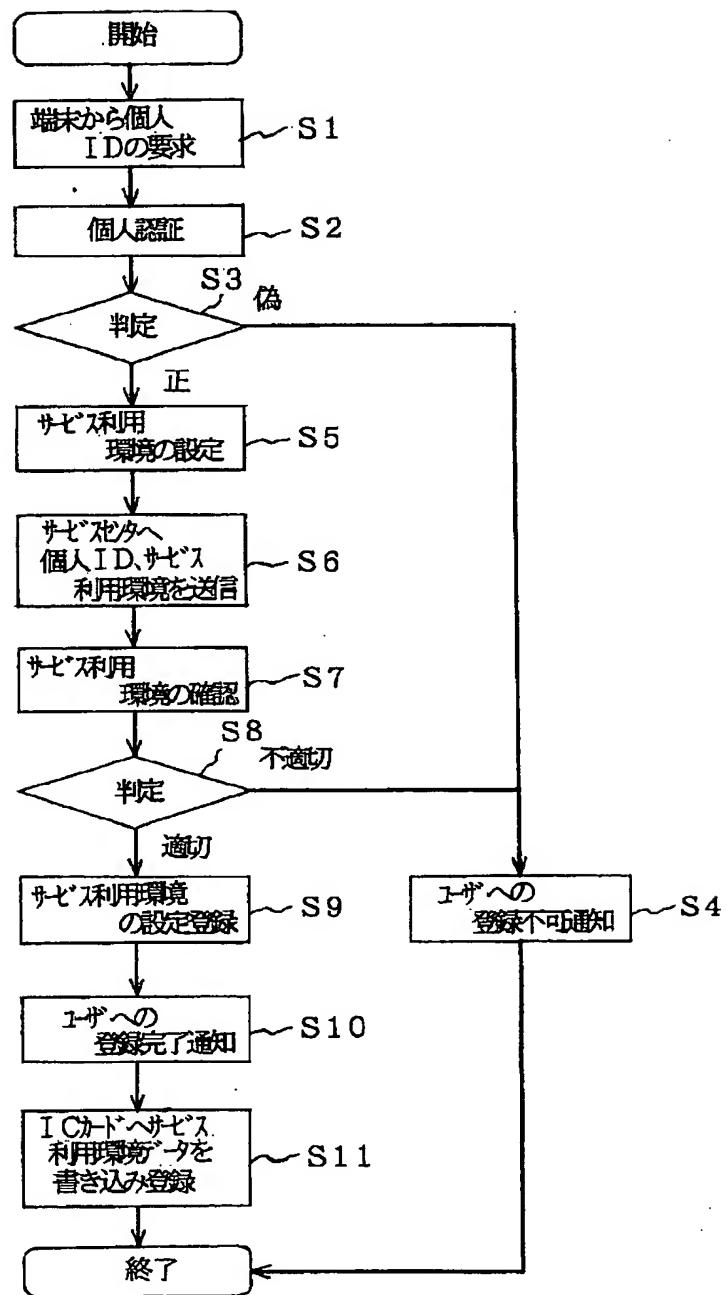
【図8】

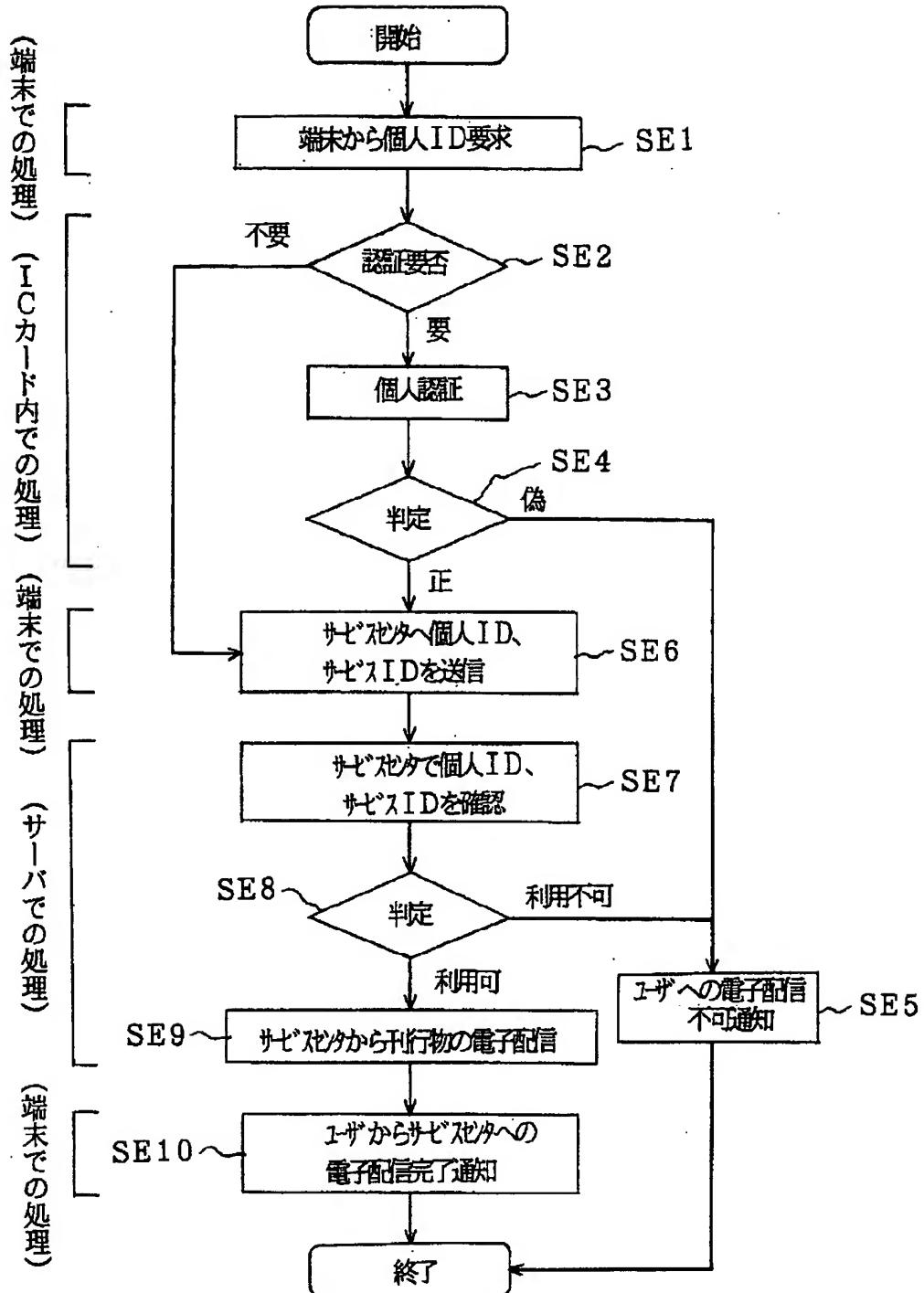


【図10】

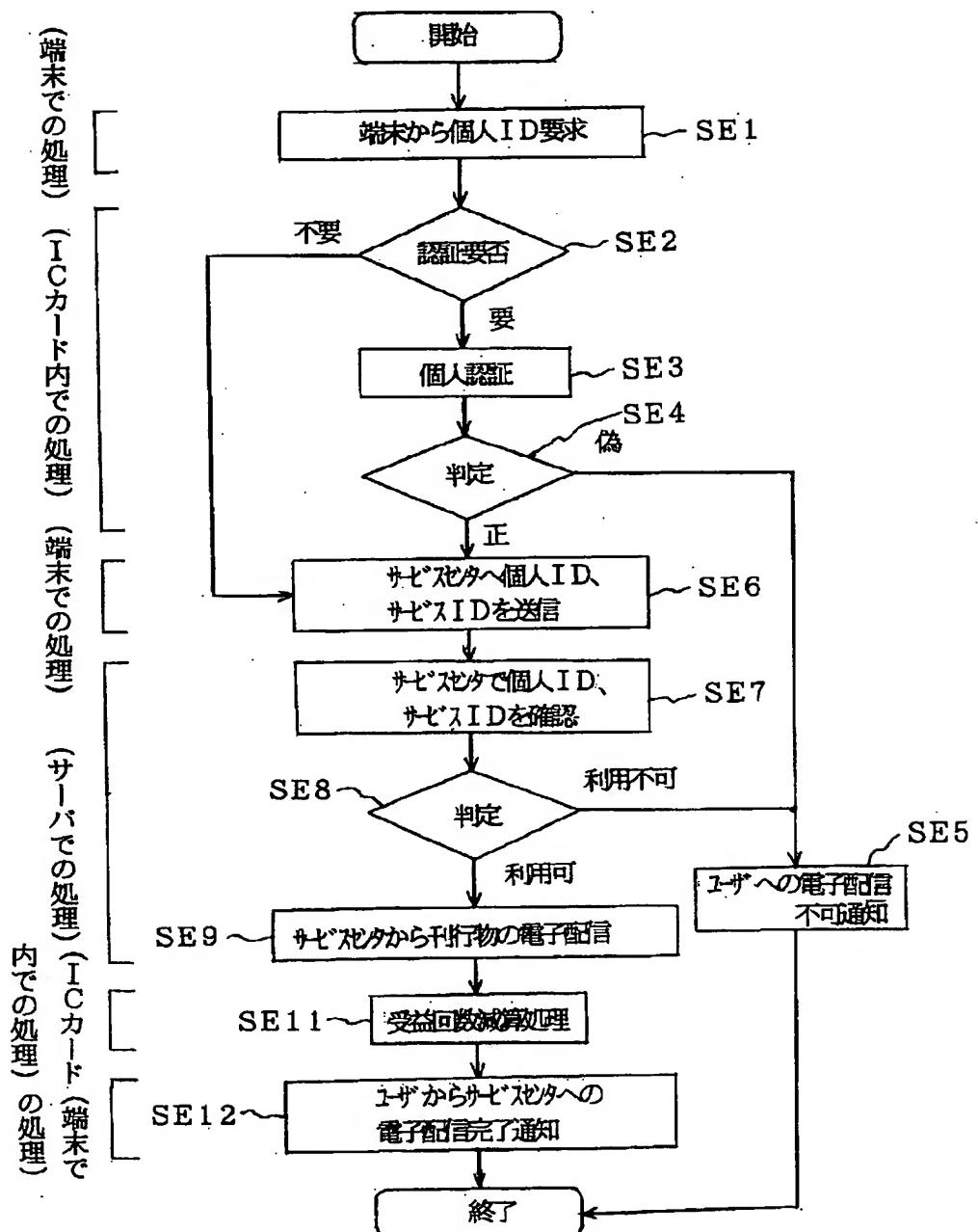


【図11】

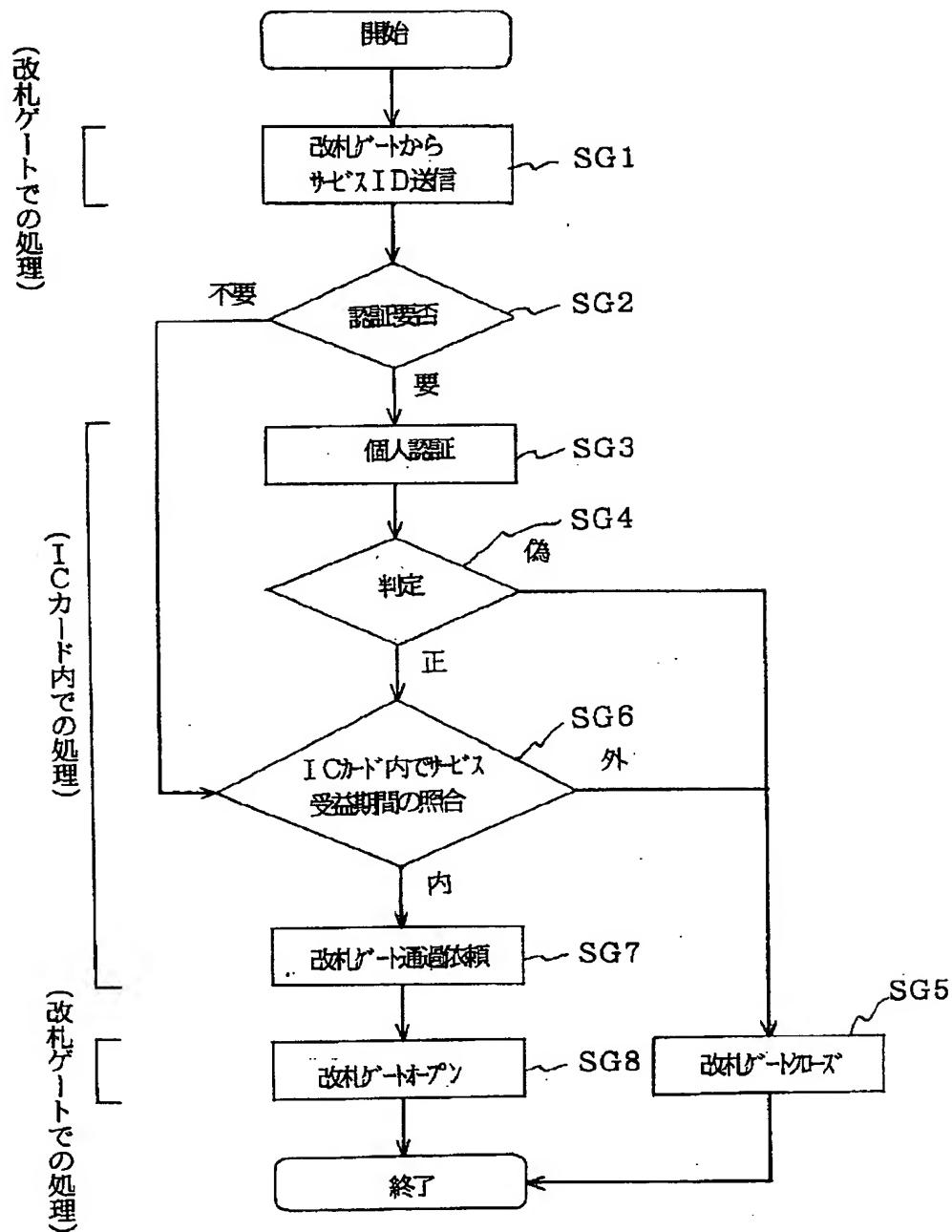




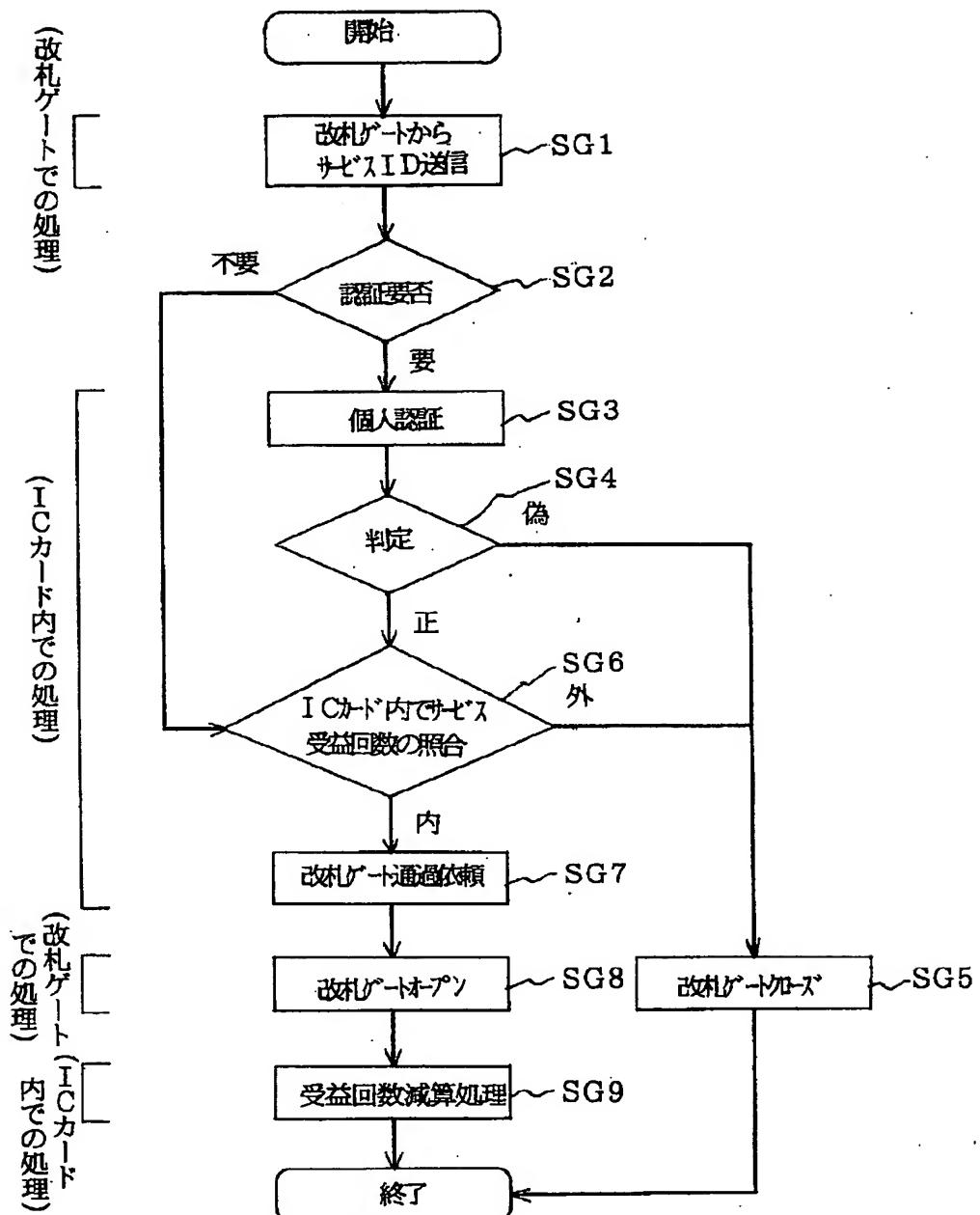
【図13】



【図14】



【図15】



フロントページの続き

(51) Int. Cl. 6  
G 06 K 19/073

識別記号

F I  
G 06 K 19/00

P

(72) 発明者 加藤 喜久次  
東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内